DECLARATION

I, Gwendoline Bruneau, a patent agent, residing at 2052 Saint Andre, Montreal, Quebec, Canada, H2L 3V1, hereby declare that I am thoroughly acquainted with the French and English languages and that the attached translation is a true translation of the Canadian Patent Application CA 2258809.

AND I HAVE SIGNED

Gwendoline Bruneau

SWORN to and subscribed before me this
1 day of August, 2005.

Commissioner for Oaths

TITLE OF THE INVENTION

COMPUTER GAMES OF CHANCE AND GAMBLING

FIELD OF THE INVENTION

The present invention relates to games of chance and gambling. More specifically, the present invention is concerned with games of chance and gambling to be played on a personal computer.

BACKGROUND OF THE INVENTION

Games of chance and gambling are conventionally controlled by an operator, such as, for example, a lottery corporation. In any cases including traditional lotteries, instant play lotteries (also called "scratch & win" lotteries), casino games and video lotteries, the operator foresees every aspect of the game, such as: collecting the wagers, issuing tickets or receipts, executing the draw, paying the winners, etc. Such control is required to ensure the integrity of the game and to eliminate any possibility of fraud.

The increasing availability and performance of personal computers have brought new possibilities for games of chance and gambling. However, a personal computer, directly controlled by the user thereof, may not be sufficiently secure for implementing games of chance and gambling while maintaining the game integrity.

Solutions to this problem have been proposed by Kaye in two related United States patents both entitled "Personal Computer Lottery Game": No. 5,569,082, issued on October 29, 1996 and No. 5,709,603 issued on January 20, 1998, which use a code determining the outcomes of a game. Such solutions involve a so-called secured supporting medium, which is not fully described in the above-mentioned documents in such a way as to solve every underlying problem.

OBJECTS OF THE INVENTION

An object of the present invention is therefore to provide an improved game of chance and gambling to be played on a computer.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram generally illustrating a general mode of operation of the method of the present invention;

Figure 2 is a block diagram of illustrating the method as per the player's viewpoint;

Figures 3, 3A and 3B form a block diagram illustrating the detailed operation of the game;

Figures 4 and 4B form a block diagram illustrating a publication operation of a new game;

Figures 5 and 5A are schematic views of a lottery ticket.

DETAILLED DESCRIPTION OF INVENTION

In order to benefit from such a sophisticated interface as offered by a computer (multimedia display, interaction with a player), the present invention allows selling games of chance and gambling to be played on a personal computer while maintaining a full control by the game operator, i.e. the national Lottery corporation.

Such control is ensured by using traditional instant type lottery ticket ("scratch & win"). These tickets contain, on a region thereof protected by a latex layer, a code, referred to hereinafter as the "Initiator Code", which allows controlling a game launched on a player's personal computer. The Initiator Code is entered in the computer by the player upon launching the game and determines the game workflow up to the final outcome thereof. The Initiator Code determines the game outcome whatever the interaction with the player. Thus, the ticket containing the Initiator Code

may be associated with a gain in advance, this gain corresponding exactly to the outcome determined when the Initiator Code is entered.

By validating the ticket, the player may claim the gain in case he won the game, as is the case with traditional lottery tickets. All risks associated with frauds occurring during playing the game on the computer are eliminated by the present invention, since the ticket is payable to the bearer.

The invention pays a particular attention to solving a number of problems, including:

- errors on the player's part: game played with a ticket that does not correspond or vice versa, error in entering the Initiator Code, etc;

- differences between an outcome announced by the game on the computer and the gain associated with the corresponding lottery ticket;

- operation errors: issuing the gains, fraudulous claims, the player's not conforming to the game outcome, etc.

- hacking aiming at uncovering valid Initiator Codes enabling play for free (business integrity);

- risks that valid Initiator Codes be translated and published, thereby allowing games for free;

- risks of uncovering valid Initiator Codes by trial and error thereby allowing games for free; and

- monitoring distribution of tickets and gains claims.

Moreover, the invention allows optimizing the flexibility of the computer means by eliminating all constraints between the Initiator Code and the possible game scenarios on the computer. Indeed, the Initiator Code does not contain any information allowing decoding the game workflow or its final outcome. Instead, the Initiator Code identifies an "initial" game value, referred to hereinafter as a "Seed", which allows controlling the game

workflow. Even the Seed itself does not contain, encoded in its value, the explicit description of the game workflow nor of the game outcome. The complete game workflow depends on the initial Seed but it cannot be deduced from the game workflow itself. Only when the Seed is "played" is the associated game workflow known.

Such an open approach, i.e. which does not force any constraint on the Initiator Code or on the Seed, allows a number of advantages, as follows:

- the Initiator Codes may be determined without taking into account the number of games in circulation, the number of target gains or any parameters of the game, which may all become constraining;

- an analysis of the Initiator Codes does not yield any information on how to generate valid Initiator Codes;

- the relation between the Initiator Codes and a Seed, and therefore the outcome of a game, is random and cannot be foreseen;

- the Seeds have a format independent of the games and of parameters governing the game workflow, which allows the invention to be applicable to any type of games;

- the relation between the Seed and the game outcome, therefore the gain in case the game is successful, is a one-way relation, i.e. it is not possible to deduce the Seed from a given outcome of a game; this feature maintains the random characteristic of used Seeds: Seeds used for a game can therefore not be inferred from the structure of the announced gains.

A preferred embodiment of the present invention will now be described as a way of illustration.

Referring to the bloc diagram of Figure 1, a general mode of operation according to a preferred embodiment of the present invention will now be described.

In block 101, a computer program, contained in a secured server, generates data necessary to the emission of a new game according to parameters (number of games, structure of the gains, etc.). This generation process yields a set of initiator Codes on the one hand and game Seeds on the other hand. The Initiator Codes are uniquely connected to each Seed.

In block 102, the Initiators Codes generated in block 101 are printed in traditional instant type lottery tickets. The Initiators Code replaces, on the surface under the latex coating of the ticket, symbols to be matched usually found there.

In block 103, the Seeds generated in block 101 are shuffled and stored, in a computer file. This file is written under the form of look-up table on cede ROMs, referred to hereinafter as CD, containing the game programs themselves.

The steps described in blocks 101, 102 and 103 will be described in more details in relation to figures 4 and 4A.

Then the tickets and the CDs are distributed using a standard lottery sales network (block 104). Kits containing CDs and tickets may be sold, or tickets alone may be sold to players already having the CDs.

Once the player has a CD and at least one ticket, the player installs the computer game contained in the CD on its computer and starts it (block 105). Following the game instructions, the player enters the Initiator Code located on the lottery tickets he bought with the CD. He is allowed one game for each purchased Initiator Code. At the end of each game, the program notifies the player and invites him to have his ticket validated in case he wins.

The player returns the winning lottery tickets to the retail establishment. The retailer then validates the tickets and gives the player his gain (block 106).

Turning now to Figure 2, which details blocks 104-106, the process as experienced by the player will now be described.

In block 201, the player purchases one or more identified lottery tickets at a conventional retail establishment. If it is his first time playing the game, the player also buys the game CD, if not, he needs only buy tickets. Since a plurality of games may be available, the CDs and tickets are clearly identified as corresponding to a given game, with corresponding "names" and "images".

Then the player, in block 202, installs the game contained in the CD on his personal computer as well known. Among the installation parameters, the player may optionally be offered to install an access control routine to limit the access of the computer gambling game, to prevent other family members, such as, for example, children, to play the game, or other persons sharing the same computer.

When ready, the game is launched, the CD still in the computer reader. The game program goes through a number of verifications, including the integrity of the CD or of certain parameters contained thereon (such as for example the Seeds look-up table, described hereinafter in block 415).

The game is identified by means of a name and images. The player may thus recognize that the started game is the one corresponding to the lottery tickets he is about to play (see Figures 5 and 5A). In block 203, the game program prompts the player to scratch the latex (see 501, Figure 5) of a lottery ticket he has and to enter the Initiator Code located thereunder (see 506, Figure 5a) into designated spaces displayed in the screen of the PC. In order to reduce the risks of mistyping on the computer keyboard, the program provides a keypad to be used with the mouse on the screen. Moreover, the Initiator Code may contain symbols that are not available on a standard computer keyboard. Such unusual symbols, varying for each game, allow ensuring that an Initiator Code is not entered for a wrong game, since the player is not able to type the symbols indicated on its tickets by means of its computer keyboard. Using such symbols alternating with letters may thus reduce the errors of simple entry (for example, the position "two" of the initiator code entered as the position "three"). In an alternative embodiment, the ticket may comprise a second latex surface containing symbols (see 503,

Figure 5) for a secondary code. When prompted by the game program, the player is to scratch this second surface containing the secondary code and enter the symbols thus uncovered (see 507, Figure 5A). These secondary symbols form part of the total value of the Initiator Code.

Once the player confirms he has finished entering the Initiator Code, the game program analysis and validates the entered Initiator Code (block 204). The Initiator Code, which has been entered under the form of symbols, is converted into a binary format for being analyzed. Some of the bits of the Initiator Code may be data allowing verifying that there was no error in entering the symbols ("check digit"). Then the Initiator Code is processed to yield an index in the look-up table of the Seeds contained in the game CD. The index allows identifying which of the Seeds of the look-up table the game program will use to control the workflow of the game and the final outcome thereof. The index further comprises, besides the Seed, data for extra validation, which ensure that the entered Initiator Code is correct and thereby reduces the odds of entering a valid Initiator Code by mere trial and error.

Once the game program has thus validated the entered Initiator Code, it starts the game by using the Seed pointed out by this Initiator Code as a starting value (block 205). This Initiator Code determines the workflow of the game and its outcome. Depending of the type of game, the player may be asked to participate in or not. Whatever his participation, the game ends by the final outcome determined in the starting Seed.

At the end of the game, the game program announces to the player in block 206, the final result, i.e. the outcome of the game. The player may be a winner or a looser. The gains may have different matures: extra game time, free games, goods, money, etc...

In block 207, in case when the player is a winner, the player keeps the lottery ticket containing the Initiator Code of the game and brings it back to the retail establishment.

The retailer validates the ticket using the traditional validation system of the Lottery, and gives the player his gain according to instructions received from the validation system (block 208).

It is to be noted that steps of blocks 203 to208 will be described in more details in relation to Figures 3, 3A and 3B.

Turning now to Figures 3, 3A and 3B, a detailed operation of the game will now be described.

Block 301 is similar to block 203 described hereinabove and relates to the scratching of the latex surface of the Lottery ticket and the entering of the Initiator Code.

In block 302, the Initiator Code is converted, from the symbols on the ticket, to binary value, to provide programming flexibility of the game. The symbols may be letters, numbers, or any other identifiable symbols, such as symbols found on playing cards, geometrical symbols, simple or stylized figures. Depending on the number of possible plays of a game and therefore on the number of printed lottery tickets, the Initiator Code has a varying length allowing covering the set of possible values. For example, an Initiator Code comprising three letters of the alphabet (A-Z) only allows 26*26*26= 17567 different Initiator Codes. To provide hundreds of thousands of tickets for a game, the Initiator Code therefore needs to be sufficiently large. In an alternative embodiment, values of an Initiator Code may be re-used on a plurality of tickets. However, all tickets having the same Initiator Code provide the same game workflow and the game same output.

In order to reduce risks of playing for free, it must be made difficult to compute or deduce an Initiator Code corresponding to a Seed in the Seed look-up table of the CD. Since the Initiator Code is related to the Seed of the game, a one-way algorithm must be used (block 303), i.e. an algorithm that can be easily use in one direction (from Initiator Code to Seed) but not on the reverse direction (from Seed to Initiator Code). The index of the Seeds look-up table is thus obtained by applying a one-way algorithm to the Initiator Code

(or to part of the Initiator Code). Among available techniques, "Exclusive OR" with strings of random bits may be used, or public key encryption algorithms such as RSA or DSA, or Digital digest algorithms like MD5 or SHA. Whatever algorithm is used, when applied to the Initiator Code it always yields a unique result for the set of possible Initiator Codes of the game. There must be a one to one relationship between each Initiator Code and each Seed of the look-up table of the game CD. The selection of an algorithm may also affect the generation of Initiator Codes (see detailed description of Figure 4). Depending on the algorithm, in certain case, the length of the Initiator Code may have to be increased to allow uniqueness of the results (in such occurrence, only Initiator Codes yielding different results are selected).

The index obtained from the Initiator Code at block 303 is used to identify an entry of the Seeds look-up table in the CD at block 304. To reduce facility of decoding this entry, it is scrambled, i.e. transformed at the binary level, by an algorithm that uses the corresponding Initiator Code as entry. Once again, standard algorithms such as DES or RC4 may be used to scramble the entry of the look-up table, the Initiator Code or part thereof being used as an encrypting key. A message digest may also be generated from the Initiator Code, and an "EXCLUSIVE OR" of the result may be done with the entry of the Seeds look-up table to scramble it. The point is to use the Initiator Code in this scrambling so that it may not be possible to unscramble the entry without knowledge of the original Initiator Code associated with the Seed during the process of creation of the game (see Figure 4). The only way out is therefore to systematically try all possible Initiator Codes.

The unscrambled entry of the Seed look-up table contains the Seed itself, a code for a gain, and data for validation of the Initiator Code. The data for validation of the Initiator Code may be total or partial digests of the original Initiator Code (MD5, SHA, etc.). Validating the Initiator Code (block 305) is done by applying again the validating algorithm to the Initiator Code entered by the player and comparing the result with the data in the Seed look-up table. The Initiator Code itself may contain verification bits ("checks bits").

At block 306, the game program thus validated the entered Initiator Code using the data in the look-up table, and in cases the results are negative, the player is prompted to enter the Initiator Code again (block 307). A wrongly entered Initiator Code or an Initiator Code randomly attempted necessarily generates an index in the Seed look-up table (303). The probabilities that this index contains validation data identifying by chance the entered Initiator Code depend on the algorithms used in blocks 302-304, and on the length of the validation data in block 305.

Obviously, the message displayed in case of a wrong entry (block 3070 does not precisely indicate which symbol of the Initiator Code is wrong, nor any reason for the wrong entry, in order not to facilitate the work of somebody trying to found valid Initiator Codes by trial and error.

When the validations of block 306 are completed, the game program uses the Seed of the entry pointed at by the entered Initiator Code to "simulate the game" a first time, without the player beware aware of it (block 308). Thanks to the power of available computer nowadays and without having to display the game workflow to the player, this process is sufficiently short be un-noticed by the player. At block 309, the outcome of this simulated game is compared with a gain code contained in the entry of the Seed obtained in 305. The gain code is a binary value corresponding to a possible outcome of the game. A code of a sufficient length is used so as to enable encoding all possible outcomes. This gain code being shuffled in the seed look-up table, it is not possible to identify which entry generates winning outcomes.

In the event the outcome of the simulated game does not match the gain code, the player is asked to enter his Initiator Code again (block 307). This allows ensuring the integrity of the Seed of the entry (i.e. ensures that there is no reading or handling error), and further reduces the probabilities to miss an error in the entered Initiator Code. Indeed, the Seed and the gain code being scrambled by the Initiator Code, the odds of having an Initiator Code valid in 306 and on the gain, the Initiator Code not being the original corresponding Initiator Code, are very poor.

Once the validation is done, the game program launches a game by using the Seed identified by the Initiator Code (block 310). The game workflow comprises an initial state and state changes leading to a final state where the game is over and cannot be played further. Each state change from the initial state is dictated by the Seed identified by the Initiator Code. The game processor generating the state changes from the initial Seed is made on the model of an algorithm of pseudo random generation, meaning that each state depends on a non –reversible fashion on the sequence of all preceding states from the initial Seed on. Thus the Seed cannot be obtained from the game workflow or from the game outcome. This technique involves a specific generation process for all the games (as described in Figure 4), and reduces the probabilities of generating valid seeds and/or a given outcome. This technique further allows dissociating the format of the Seed from the game parameters. Such flexibility allows applying the technique to any type of games.

The positioning of the game at the final state and/or the build-up of events during the game workflow (for example the build-up of game symbols or points or credits) is used to determine the close of the player's game, i.e. whether he wins or not (block 311).

The game program notifies the winning player, at block 312, that his ticket is to be returned to the retailer for validation and claiming the gain. In this regard, the ticket is a traditional lottery ticket, as provided by all Lotteries around the world.

At block 313, the lottery retailer (hereinafter referred to as the "operator") validates the ticket via a bar code or any similar or equivalent code thereon (see 502, Figure 5) and via a terminal connecting the operator to a validation system of the Lottery. In case the operator does not have access to such a terminal, he may sue special codes located on a specific zone of the ticket (see 504, Figure 5) to determine whether the ticket is a winning ticket or not, and if it is, to determine the nature of the gain. In that case, the ticket is then to be transmitted to a validation center of the Lottery.

Given the links between the Initiator Code of the ticket, the Seed of the game determining the outcome thereof, and the bar code uniquely identifying the ticket, the validation system of the Lottery knows the outcome of each played game. A centralized database of the Lottery (generated during the process illustrated in Figure 4) establishes a link between the bar codes of the tickets and the gains corresponding to the Initiator Code. The Initiator Code itself is not maintained in this database, nor the Seed of the corresponding game, for security reasons (the staff of the Lottery is thus unable to publish valid Initiator codes nor Seeds). Only the winning tickets of a batch are maintained therein. That is why, in block 314, the Lottery system uses the database to determine whether the ticket is a winning ticket.

At block 315, the Lottery system determines whether the bar code of the ticket correspond to an entry of the Lottery database. If yes, the ticket corresponds to a winning Initiator code (end hence to a winning Seed), and a semaphore indicates whether the ticket has already been claimed. If no, the ticket is not a winning ticket. Such procedures are standard procedures as known with traditional lottery tickets.

In the case when the ticket is a non-winning ticket (block 316) or when it has already been claimed or when the bar code is invalid (the bar codes contain integrity validation data), the operator's terminal displays and prints a corresponding message.

In the case when the ticket is winning ticket and therefore non-yet claimed (block 317), it is then noted as "claimed" in the data base. Such standard security procedure ensures that winning tickets are only claimed once. Then, in block 318, a message indicating the gain corresponding to the ticket is transmitted to the operator's terminal for display and printing. The operator, at block 319, then gives the indicated gain to the player and destroys the ticket ("cash&trash").

Finally, the lottery system is notified that the player has been given his gain by the operator and credits the operator with a corresponding amount (block 320).

Turning now to Figures 4 and 4A, the publication of a new game will now be described.

Any new game is planned before being launched on the market. The number of tickets (and thus the number of games) emitted for sale and the structure of the gains, i.e. the portion of the sales returned to the players as gains, have to be determined. As is the case with traditional instant Lottery, the game operator, i.e. a National Lottery Company, referred to hereinafter as the "Lottery", defines all these parameters, as well as features involved during the game and its workflow. For example, it may be decided that the workflow incorporates an apparently high gain probability for the player ("near miss"). All these parameters s well as a detailed structure of the gains, are encoded in a computer file at block 401.

A program of the Lottery uses the game generator (see blocks 310 and 311) to identify Seeds yielding results corresponding to the parameter file defined in 401. At block 401, the program randomly generates game Seeds and plays them. For each such played games, it compares the results, i.e. each step of the workflow and the outcome, with the results corresponding to the parameter file defined in 401. This process may proceed by incrementation from an initial Seed, or by jumps, and generates a set of distributed Seeds.

Each time the program obtains a Seed yielding desired results, this seed is saved in a file together with its corresponding game output (block 403). The parameter file is updated to indicate which results are obtained. More than one Seed for a desired result may be saved, thereby providing a larger batch of Seeds and Initiator codes for sale.

When all parameters are satisfied, the file containing the Seeds and the outcomes is randomly shuffled and put in a look-up table containing an entry per Seed (block 404). The random shuffling allows dissociating the seed generation process from the seed sequence in the final look-up table. As a result, even a programmer familiar the above-mentioned

process cannot track a Seed in the Look-up table knowing its position (block 402).

To further securing the Seed table against computer fraud ("hackers"), false entries are introduced, in block 405, which are entries not corresponding to any valid Seed or Initiator Code. For an efficient security, the number of false entries should be has high as the number of valid entries. False entries are in fact strings of randomly generated bits. These false entries are randomly distributed among valid entries.

An index for an entry corresponds to its position relative to he beginning of the look-up table. For example, the index of a valid Seed located in 3145th position in the Look-up table is 3145. The valid Seeds being mixed with false ones, indexes are not continuous. A non-reversible algorithm is then used, in block 406, to obtain a bootstrap value X that yields as an output the index in binary value. For example, the binary value, which encoded by an algorithm such as DES, used as a coding key, gives the index value, may be determined (the index value may be extracted from the result in case the result is longer than the index). Such process being essentially trial and error based, it may take quite a long time. Therefore, a more global approach may be contemplated, whereby results fro different bootstrap values X are produces in series and then the results among them satisfying the desired indexes are selected. Some algorithms are easier to use than others. For example, if the index is given as a binary value of 20 positions, a bootstrap value X of 40 bits may be easily generated, which, by addition of two halves thereof by an "EXCLUSIVE OR" yields the desired index. This bootstrap value X may be determined from the index as follows: the first 20 bits are randomly generated, the 20 last bits are generated by applying an "EXCLUSIVE OR" to the 20 first bits and the index value itself. Alternatively, public key encrypting algorithms may be used, the bootstrap value X being then generated by using a private key on the index, the index being obtained from the bootstrap value X using the public key. However, using public key encrypting algorithms involves using relatively long bits strings.

In block 407, T=the bootstrap X value obtained in 406 for each Seed of the Look-up table is entered. This value is used for validating the Initiator Code of a real game. As the Initiator Code corresponds to the bootstrap value X with a symbol format adequate for the ticket, finding it in the entry of the Seeds look-up table ensures that the Initiator Code is indeed that generated by the Lottery and not an "alias" that would yield similar results upon application of non-reversible algorithms described in relation to blocks 303-305. Using one way algorithms cannot ensure that another input value (Initiator Code) does not yield the same output (index), hence the use in comparing the original value of the Initiator Code saved in the Seeds look-up table.

For each valid Seed, the bootstrap value X is then translated under the form of an Initiator Code, i.e. as a strings of symbols that are eventually printed on a Lottery ticket (block 408). The correspondence between the symbols and the binary values may be varied from on game to another game, and even from one position of the Initiator Code to a following one. Part of the Initiator Code may be under the form of a look-up table of several symbols (see 5-3 Figure 5). In such case, the game program only asks, randomly, one symbol from this look-up table (each symbol being mathematically related to a number of a position of the look-up table so as to always correspond to a same result in binary value). Such approach allows reducing the risks that Initiator Codes be translated and published allowing players to play for free. Indeed, the translation is quite lengthy since the number of data to be translated is increased, which may deter such players.

To allow validation by the Lottery system, each Initiator Code is then associated with a unique ticket number at block 409. This unique number is independent from the Initiator Code itself, in such a way that one cannot be deduced form the other. This association is usually performed by a printer in charge of printing the Lottery tickets. Thus the Lottery staff has no access to this association process.

Then printing of instant type Lottery tickets is performed, whereby the surface under a latex coating is replaced by the symbols

corresponding to the Initiator Code (block 410), The printed Lottery tickets are then distributed on traditional sale networks of the Lottery (block 411). Part f these tickets are packaged together with a game CD. The remaining part is sold by itself.

The unique number of each winning ticket (in the bar code of the ticket, see 503 Figure 5) is stored together with the amount of the gain in the database of the centralized validation system of the Lottery (block 412). In the case when the bar code is associated with the Initiator Codes and hence to the gains) by the printer, the Lottery provides these information to the printer. The Initiator Codes are not contained in this database. Tickets containing non-winning Initiator Code are not listed in this database. Upon validation of the tickets, a bar code that is not listed in the database is automatically considered as non-winning.

As mentioned hereinabove, the tickets database (see block 413) is used by the Lottery traditional validation system. The sale network of the Lottery allows each retailer operator to use a validation terminal connected by a network to this central system.

As the Look-up table of Seeds is contained in the game CD, its content has to be protected to prevent a hacker from calculating the Initiator Codes or Seeds allowing playing games for free. In block 414, each entry of the Look-up table of Seeds is separately shuffled by using a reversible algorithm (allowing unshuffling). Such algorithm uses the Initiator Code entry to vary the shuffling from one entry to another entry and make the unshuffling difficult in absence of knowledge of the original Initiator Code associated with the entry. For example, a MD5 or SHA digest of the Initiator Code may be generated (the digest being length to satisfy the minimum length required by the algorithm) and the result applied as an "EXCLUSIVE OR" upon the entry containing the Seed and the validation data (X value block 407 and gain code block 404). Thus, the original Initiator Code is needed to unshuffle the entry.

The shuffled Look-up table of Seeds is copied on each CD distributed together with the ticket (block 405). This CD also contains the

game program itself. A total digest of the Look-up table (MD5 or SHA) may also be added on the CD to further secure the production of the CD. This digest is then verified upon launching the game (block 202).

The CD (block 416) are packaged with tickets (block 411) ready for distribution, or separately sold. The CD being devoid of any cash-in value, they may be distributed for free as a way to stimulate the sale of tickets allowing playing the game.

Figures 5 and 5A, described in details hereinafter, illustrate an embodiment of a Lottery ticket according to the present invention.

The Lottery tickets are of the standard instant type ("scratch & win"). Figure 5 shows a unscratched ticket 505, i.e. comprising a latex coating 501 covering the Initiator Code, while Figure 5A illustrates the same ticket one after this latex coating 501 has been scratched by the player.

The surface on which the Initiator Code is printed is protected by the latex coating 501 so that wining tickets may not be spotted before they are purchased. A scratched ticket cannot be sold. Latex coating is widely used in Lotteries and is efficient against a number of techniques aiming at reading under the surface (using illumination, chemical processes, scratching and gluing etc.). A colored pattern (not shown) is typically printed on the latex coating 501 in order to make any attempts of fraud or counterfeiting difficult.

The bar code 502 of the ticket contains a number uniquely identifying each ticket for a given game. This number may be encoded with a hierarchy of data: game number, booklet number, publication number, etc... A number of standard bar codes formats may be used depending on the length of the encoded number (128c). Denser so-called two-dimensional formats may also be used. Bar codes usually contain flag values allowing detecting reading errors. Moreover, this number itself may contain other verification values allowing for an integrity control until the ticket is received for validation to the central validation system of the Lottery.

The surface 507 of the ticket may comprise varied symbols. Such a surface is optional. It allows supporting part of the Initiator Code under a format that is not easily deciphered. Although only a single position of this surface is used as an entry by the player, the Look-up table as a whole is to be available since the game program selects a position at random during the game. The more numerous the positions, the more difficult it is to decipher the information contained on the ticket to have it handy for publishing and use for a play for free only. A latex layer 503 covers the surface 507.

The latex coating 504 is a common feature in Lottery tickets. It covers the bar codes that allow the Lottery operators to identify a wining ticket and an associated gain without having to refer to the central system of the Lottery. This information is used in case the validation system is non available or when fraud is suspected. This surface is never to be scratched by the player.

The remaining part of the ticket 505 is typically printed in color with pattern illustrating the theme of the game. Besides making counterfeiting uneasy, this allows linking the tickets with the game itself (and with the CD).

Symbols of the Initiator Code 506 may be provided in several ways depending on the number of symbols required. Non-alphanumerical symbols may be explained by a short small-character description to avoid any confusion. For example, the symbol of scissors may be labeled with the word "scissors".

Although the present invention has been described hereinabove by way of preferred embodiments thereof, it can be modified, without departing from the spirit and nature of the subject invention as defined in the appended claims.

CLAIMS

1. A game of chance to be played on a computer, comprising:

an instant type lottery ticket bearing an Initiator Code and a code;

a computer program including means for reading the Initiator Code thus revealing a Seed; an algorithm allowing obtaining the game workflow and the game output from the Seed; and a game embodying the game workflow and the game output for a player.